Introducing Digital Evidence in California State Courts[i]

Introducing Documentary and Electronic Evidence

In order to introduce documentary and electronic evidence obtained in compliance with California Electronic Communication Privacy Act (Penal Code §§ 1546.1 and 1546. 2) in court, it must have four components: 1) it must be relevant. 2) it must be authenticated. 3) its contents must not be inadmissible hearsay; and 4) it must withstand a "best evidence" objection.

If the digital evidence contains “metadata” (data about the data such as when the document was created or last accessed, or when and where a photo was taken) proponents will to need to address the metadata separately, and prepare an additional foundation for it.

I. Relevance

Only relevant evidence is admissible. (Evid. Code, § 350.) To be "relevant," evidence must have a tendency to prove or disprove any disputed fact, including credibility. (Evid. Code, § 210.) All relevant evidence is admissible, except as provided by statute. (Evid. Code, § 351.)

For digital evidence to be relevant, the defendant typically must be tied to the evidence, usually as the sender or receiver. With a text message, for example, the proponent must tie the defendant to either the phone number that sent, or the phone number that received, the text. If the defendant did not send or receive/read the text, the text-as-evidence might lack relevance. In addition; evidence that the defendant is tied to the number can be circumstantial. And evidence that the defendant received and read a text also can be circumstantial.

Theories of admissibility include:

- Direct evidence of a crime
- Circumstantial evidence of a crime
- Identity of perpetrator
- Intent of perpetrator
- Motive
- Credibility of witnesses
- Impeachment
- Negates or forecloses a defense
- Basis of expert opinion
- Lack of mistake

II. Authentication

To "authenticate" evidence, you must introduce sufficient evidence to sustain a finding that the writing is what you say it is. (Evid. Code, § 1400 (a).) You need not prove the genuineness of the evidence, but to authenticate it, you must have a witness lay basic foundations for it. In most cases you do this by showing the writing to the witness and asking, "what is this?" and “how do you know that?” It is important to note that the originator of the document is not required to testify. (Evid. Code, § 1411.)

The proponent should present evidence of as many of the grounds below as possible. However, no one basis is required. Additionally, authentication does not involve the truth of the document’s content, rather only whether the document is what it is claimed to be. (*City of Vista v. Sutro & Co*. (1997) 52

Cal.App.4th 401, 411-412.) Digital evidence does not require a greater showing of admissibility merely because, in theory, it can be manipulated. Conflicting inferences go to the weight not the admissibility of the evidence. (*People v. Goldsmith* (2014) 59 Cal. App.258, 267) *In Re KB* (2015) 238 Cal.App.4th 989, 291-292 [upholding red light camera evidence].) *Goldsmith* superseded *People v. Beckley* (2010) 185 Cal. App.4th 509, which required the proponent to produce evidence from the person who took a digital photo or expert testimony to prove authentication. Documents and data printed from a computer are considered to be an "original." (Evid. Code 255.)

Printouts of digital data are presumed to be accurate representation of the data. (Evid Code §§ 1552, 1553.) However, that presumption can be overcome by evidence presented by the opposing party. If that happens, the proponent must present evidence showing that by a preponderance, the printouts are accurate and reliable. (*People v. Retke* (2015), 232 Cal. App. 4th 1237 [successfully challenging red light camera data].)

A. You can authenticate documents by:

- Calling a witness who saw the document prepared. (Evid. Code, § 1413.)
- Introducing an expert handwriting comparison. (Evid. Code, § 1415.)
- Asking a lay witness who is familiar with the writer's handwriting to identify the handwriting. (Evid. Code, § 1516.)
- Asking the finder of fact (i.e. the jury) to compare the handwriting on the document to a known exemplar. (Evid. Code, § 1470.)
- Showing that the writing refers to matters that only the writer would have been aware. (Evid. Code, § 1421.)
- Using various presumptions to authenticate official records with an official seal or signature. (Evid. Code, § 1450-1454.) Official records would include state prison records, Department of Motor Vehicle documents or documents filed with the Secretary of State. There is a presumption that official signatures are genuine. (Evid. Code, § 1530, 1453.)
- Any other way that will sustain a finding that the writing is what you say it is. The Evidence Code specifically does not limit the means by which a writing may be authenticated and proved. (Evid. Code, § 1410; *See also People v. Olguin* (1994) 31 Cal.App.4th 1355, 1372-1373 [rap lyrics authenticated in gang case even though method of authentication not listed in Evidence Code].)

B. Common ways to authenticate email include:

- Chain of custody following the route of the message, coupled with testimony that the alleged sender had primary access to the computer where the message originated.
- Security measures such as password-protections for showing control of the account. (See generally, *People v. Valdez* (2011) 201 Cal.App.4th 1429.)
- The content of the email writing refers to matters that only the writer would have been aware.

- Recipient used the reply function to respond to the email; the new message may include the sender's original message.

- After receipt of the email, the sender takes action consistent with the content of the email.

- Comparison of the e-mail with other known samples, such as other admitted e-mails.

- E-mails obtained from a phone, tablet or computer taken directly from the sender/receiver, or in the sender/receiver's possession.

In the majority of cases a variety of circumstantial evidence establishes the authorship and authenticity of a computer record. For further information, please consult *Chapter 5 – Evidence* of the United States Department of Justice, Computer Crime and Intellectual Property Section Criminal Division, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (2009) <http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf> (accessed Aug. 18, 2016). See also, *Lorraine v. Markel American Ins. Co*. (D. Md. 2007) 241F.R.D. 534, 546 [seminal case law on authenticating digital evidence under F.R.E.],)

C. Common ways to authenticate chat room or Internet relay chat (IRC) communication include:

- Evidence that the sender used the screen name when participating in a chat room discussion. For example, evidence obtained from the Internet Service Provider that the screen name, and/or associated internet protocol (IP address) is assigned to the defendant or evidence circumstantially tying the defendant to a screen name or IP address.

- Security measures such as password-protections for showing control of the account of the sender and excluding others from being able to use the account. (See generally, *People v. Valdez* (2011) 201 Cal.App.4th 1429.)

- The sender takes action consistent with the content of the communication.

- The content of the communication identifies the sender or refers to matters that only the writer would have been aware.

- The alleged sender possesses information given to the user of the screen name (contact information or other communications given to the user of the screen name).

- Evidence discovered on the alleged sender's computer reflects that the user of the computer used the screen name. (See *U.S. v. Tank* (9th Cir. 2000) 200 F.3d 627.)

- Defendant testified that he owned account on which search warrant had been executed, that he had conversed with several victims online, and that he owned cellphone containing photographs of victims, personal information that defendant confirmed on stand was consistent with personal details interspersed throughout online conversations, and third-party service provider (Facebook) provided certificate attesting to chat logs' maintenance by its automated system. (*U.S. v. Br*owne (3d Cir. Aug.25, 2016) 2016 WL 4473226, at 6.)

In the majority of cases it is a variety of circumstantial evidence that provides the key to establishing the authorship and authenticity of a computer record. For further information, please consult *Chapter 5 – Evidence* of the United States Department of Justice, Computer Crime and Intellectual Property Section Criminal Division, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (2009) <http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf> (accessed Aug. 18, 2016.)

D. Common ways to authenticate social media postings include:

- Testimony from a witness, including a police officer, with training and experience regarding the specific social media outlet used testified about what s/he observed. (*In re K.B.* (2015) 238 Cal.App.4th 989.) What is on the website or app, at the time the witness views it, should be preserved in a form that can be presented in court.

- Evidence of social media postings obtained from a phone, tablet or computer taken directly from the sender/receiver, or in the sender/receiver's possession.

- Testimony from the person who posted the message.

- Chain of custody following the route of the message or post, coupled with testimony that the alleged sender had primary access to the computer where the message originated.

- The content of the post refers to matters that only the writer would have been aware.

- After the post on social media, the writer takes action consistent with the content of the post.

- The content of the post displays an image of the writer. (*People v. Valdez* (2011) 201 Cal.App.4th 1429.)

- Other circumstantial evidence including that the observed posted images were later recovered from suspect's cell phone and the suspect was wearing the same clothes and was in the same location that was depicted in the images. (*In re K.B.* (2015) 238 Cal.App.4th 989.)

- Security measures for the social media site such as passwords-protections for posting and deleting content suggest the owner of the page controls the posted material. (*People v. Valdez* (2011) 201 Cal.App.4th 1429.)

In the majority of cases it is a variety of circumstantial evidence that provides the key to establishing the authorship and authenticity of a computer record. "Mutually reinforcing content" as well as "pervasive consistency of the content of the page" can assist in authenticating photographs and writings. (*People v. Valde*z (2011) 201 Cal.App.4th 1429, 1436.) For further information, please consult *Chapter 5 – Evidence* of the United States Department of Justice, Computer Crime and Intellectual Property Section Criminal Division, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (2009) <http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf> (accessed Aug. 18, 2016.) For examples of sufficient circumstantial evidence authenticated social media posts see, *Tienda v. State* (Tex. Crim. App. 2012) 358 S.W.3d 633, 642; *Parker v. State* (Del. 2014) 85 A.3d 682, 687. Contrast, *Griffin v. State* (2011) 419 Md. 343, 356–359.

E. Common ways to authenticate web sites include:

- Testimony from a witness, including a police officer about what s/he observed. (See *In re K.B.* (2015) 238 Cal.App.4th 989.) What is on the website or app, at the time the witness views it, should be preserved in a form that can be presented in court.

- Testimony from the person who created the site.

- Website ownership/registration. This is a legal contract between the registering authority (e.g. Network Solutions, PDR Ltd, D/B/A PublicDomainRegistry.com, etc.) and the website owner, allowing the registered owner to have total dominion and control of the use of a website name (domain) and its content. (See *People v. Valdez* (2011) 201 Cal.App.4th 1429 [password protection suggest the owner of the page controls the posted material].) It may be possible to admit archived versions of web site content, stored and available at a third party web site (See https://archive.org/web/ [Wayback Machine].) First, it may be authenticated by a percipient witness who previously saw or used the site. It may also be possible to obtain a declaration or witness to testify to the archive. (See e.g. *Telewizja Polska USA, Inc. v. Echostar Satellite Corp.*, 2004 WL 2367740, at 16 (N.D.Ill. Oct.15, 2004) [analyzing admissibility of the content of an achieved website].)

The underlying challenge for web sites in not the authentication of the site; rather the content or hearsay material contained therein. In *St. Clair v. Johnny's Oyster & Shrimp, Inc*. (S.D.Tex.1999) 76 F.Supp.2d 773, 774-75 the court noted that "voodoo information taken from the Internet" was insufficient to withstand motion to dismiss because "[n]o web-site is monitored for accuracy" and "this so-called Web provides no way of verifying the authenticity" of information plaintiff wished to rely on. (See also *Badasa v. Mukasey* (8th Cir. 2008) 540 F.3d 909 [Nature of Wikipedia makes information from the website unreliable].) However, at noted in *Section III Hearsay*, the contents of the web site could be admitted as an operative fact or under a number of exceptions including an admission of a party opponent.

F. Authenticating Texts:

A text message is a writing within the meaning of Evidence Code section 250, which may not be admitted in evidence without being authenticated. (*Stockinger v. Feather River Community College* (2003) 111 Cal.App.4th 1014, 1027–1028.) A text message may be authenticated "by evidence that the writing refers to or states matters that are unlikely to be known to anyone other than the person who is claimed by the proponent of the evidence to be the author of the writing" (Evid.Code, § 1421), or by any other circumstantial proof of authenticity (*Id.,* § 1410).

As of August 2016, there are no published California cases that specifically discuss what is required for authenticating a text message. Unpublished California opinions are consistent with the rule set forth above for authenticating e-mails and chats through a combination of direct and circumstantial evidence based on the facts of the case. Because of the mobile nature of smart phones, the proponent must take care to tie the declarant to the phone from which texts were seized or to the phone number listed in records obtained from the phone company. Often this done through cell phone records or the phone being seized from the defendant, his home or car or other witnesses testifying that this was how they communicated with the defendant.

Published opinions from other jurisdictions and unpublished opinions from California provide some guidance:

- Victim testified he knew the number from which text was sent because Defendant told him the number. The contents of the texts referred to victim as a snitch. The defendant called the victim during the course of the text message conversation. [(*Butler v. State*, 459 S.W. 3d 595 (Crim. Ct App. Tx. April 22, 2015].)

- Testimony of records custodian from telecommunications company, explaining how company kept records of actual content of text messages, the date and time text messages were sent or received, and the phone number of the individuals who sent or received the messages, provided proper foundation for, and sufficiently authenticated, text messages admitted into evidence in trial on armed robbery charges. (Fed.Rules Evid.Rule 901(a), *U.S. v. Carr* (11th Cir. 2015) 607 Fed.Appx. 869.)

- Ten of 12 text messages sent to victim's boyfriend from victim's cellular telephone following sexual assault were *not* properly authenticated to extent that State's evidence did not demonstrate that defendant was author of text messages. (*Rodriguez v. State* (2012) 128 Nev. Adv. Op. 14, [273 P.3d 845].)

- Murder victim's cell phone recovered from scene of crime. Forensic tools used on phone recovered texts back and forth between victim and defendant. (*People v. Lehmann* (Cal. Ct. App., Sept. 17, 2014, No. G047629) 2014 WL 4634272 [Unpublished].)

- Defendant laid an inadequate foundation of authenticity to admit, in prosecution for assault with a deadly weapon, hard copy of e-mail messages (Instant Messages) between one of his friends and the victim's companion, as there was no direct proof connecting victim's companion to the screen name on the e-mail messages. (*People v. Von Gunten* (2002 Cal.App.3d Dist.) 2002 WL 501612. [Unpublished].)

G. Authenticating Metadata:

Another way in which electronic evidence may be authenticated is by examining the metadata for the evidence. Metadata, "commonly described as 'data about data,' is defined as 'information describing the history, tracking, or management of an electronic document.' Metadata is 'information about a particular data set which describes how, when and by whom it was collected, created, accessed, or modified and how it is formatted (including data demographics such as size, location, storage requirements and media information).' Some examples of metadata for electronic documents include: a file's name, a file's location (e.g., directory structure or pathname), file format or file type, file size, file dates (e.g., creation date, date of last data modification, date of last data access, and date of last metadata modification), and file permissions (e.g., who can read the data, who can write to it, who can run it). Some metadata, such as file dates and sizes, can easily be seen by users; other metadata can be hidden or embedded and unavailable to computer users who are not technically adept." Because metadata shows the date, time and identity of the creator of an electronic record, as well as all changes made to it, metadata is a distinctive characteristic of all electronic evidence that can be used to authenticate it under Federal Rule 901(b)(4).

Although specific source code markers that constitute metadata can provide a useful method of authenticating electronically stored evidence, this method is not foolproof because, "[a]n unauthorized person may be able to obtain access to an unattended computer. Moreover, a document or database located on a networked-computer system can be viewed by persons on the network who may modify it. In addition, many network computer systems usually provide authorization for selected network administrators to override an individual password identification number to gain access when necessary. Metadata markers can reflect that a document was modified when in fact it simply was saved to a different location. Despite its lack of conclusiveness, however, metadata certainly is a

useful tool for authenticating electronic records by use of distinctive characteristics." (*Lorraine v. Markel American Ins. Co.* (D. Md. 2007) 241 F.R.D. 534, 547–48 [citations omitted].)

F. Challenges to Authenticity

Challenges to the authenticity of computer records often take on one of three forms. First, parties may challenge the authenticity of both computer-generated and computer-stored records by questioning whether the records were altered, manipulated, or damaged after they were created.

Second, parties may question the authenticity of computer-generated records by challenging the reliability of the computer program that generated the records. California state courts have refused to require, as a prerequisite to admission of computer records, testimony on the "acceptability, accuracy, maintenance, and reliability of ... computer hardware and software." (*People v. Lugashi* (1988) 205 Cal.App.3d 632, 642.) As *Lugashi* explains, although mistakes can occur, " 'such matters may be developed on cross-examination and should not affect the admissibility of the [record] itself.' (*People v. Martinez* (2000) 22 Cal.4th 106, 132.)

Third, parties may challenge the authenticity of computer-stored records by questioning the identity of their author. For further information, please consult "Defeating Spurious Objections to Electronic Evidence," by Frank Dudley Berry, Jr., [click here] or *Chapter 5 – Evidence* of the United States Department of Justice, Computer Crime and Intellectual Property Section Criminal Division, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (2009) <http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf> (accessed Aug. 18, 2016).

III. Hearsay Rule

The first question to ask is whether or not the information within the document is hearsay. If it is hearsay, then you need an applicable exception, such as business and government records or statement by party opponent. Examples of things that are *not* hearsay include; 1) operative facts and 2) data that is generated by a mechanized process and not a human declarant and, 3) A statement being used to show its falsity not its truth.

A. Operative Facts

Where " 'the very fact in controversy is whether certain things were said or done and not ... whether these things were true or false, ... in these cases the words or acts are admissible not as hearsay[,] but as original evidence.' " (1 Witkin, Cal. Evidence (4th ed. 2000) Hearsay, § 31, p. 714.) For example, in an identity theft prosecution, there will be no hearsay issue for the majority of your documents. The documents are not being offered for the truth of the matter asserted; they are operative facts. In *Remington Investments, Inc v. Hamedani* (1997) 55 Cal.App.4th 1033, the court distinguished between the concept of authentication and hearsay. The issue was whether a promissory note was admissible. The court observed that: 'The Promissory Note document itself is not a business record as that term is used in the law of hearsay, but rather an operative contractual document admissible merely upon adequate evidence of authenticity. (*Id.* At 1043.)

Under Remington, promissory notes, checks and other contracts are not hearsay, but operative facts. Moreover, forged checks, false applications for credit, and forged documents are not hearsay. They

are not being introduced because they are true. They are being introduced because they are false. Since they are not being introduced for the truth of the matter asserted there is no hearsay issue.

Other examples of non-hearsay documents would include:

- The words forming an agreement are not hearsay (*Jazayeri v. Mao* (2009) 174 Cal.App.4th 301, 316 as cited by *People v. Mota* (Cal. Ct. App., Oct. 8, 2015, No. B252938) 2015 WL 5883710 (Unpublished)

- A deposit slip and victim's identification in a burglary case introduced to circumstantially connect the defendant to the crime. *(In re Richard* (1979) 91 Cal.App.3d 960, 971-979.)

- Pay and owes in a drug case. (*People v. Harvey* (1991) 233 Cal.App.3d 1206, 1222-1226.)

- Items in a search to circumstantially connect the defendant to the location. (*People v. Williams* (1992) 3 Cal.App.4th 1535, 1540-1543.)

- Invoices, bills, and receipts are generally hearsay unless they are introduced for the purpose of corroborating the victim's damages. (*Jones v. Dumrichob* (1998) 63 Cal.App.4th 1258, 1267.)

- Defendant's social media page as circumstantial evidence of gang involvement. (*People v. Valdez* (2011) 201 Cal.App.4th 1429.

- Logs of chat that was attributable to Defendant were properly admitted as admissions by party opponent, and the portions of the transcripts attributable to another person were properly classified as "non hearsay", as they were not "offered for the truth of the matter asserted." Replacing screen names with actual names appropriate demonstrative evidence. (*U.S. v. Burt* (7th Cir., 2007) 495 F.3d 733.)

- "To the extent these images and text are being introduced to show the images and text found on the websites, they are not statements at all—and thus fall outside the ambit of the hearsay rule." (*Perfect 10, Inc. v. Cybernet Ventures, Inc.* (C.D.Cal.2002) 213 F.Supp.2d 1146, 1155.)

- Generally, photographs, video, and instrument read outs are not statements of a person as defined by the Evidence Code. (Evid.Code §§ 175, 225; *People v. Gold*smith (2014) 59 Cal.4th 258, 274; *People v. Lop*ez (2012) 55 Cal.4th 569, 583.)

Although the check itself is not hearsay, the bank's notations placed on the back of the check showing that it was cashed is hearsay. The bank's notations would be introduced for the truth of the matter asserted – that the check was cashed. Evidence Code sections 1270 and 1271 solve this problem by allowing the admission of these notations as a business record.

Two helpful rules that apply to business records. First, it may be permissible to infer the elements of the business record exception. In *People v. Dorsey* (1974) 43 Cal.App.3d 953, the court was willing to find that it was common knowledge that bank statements on checking accounts are prepared daily on the basis of deposits received, checks written and service charges made even though the witness failed to testify as to the mode and time of preparation of bank statements. The second rule is that

"lack of foundation" is not a sufficient objection to a business record. The defense must specify which element of the business record exception is lacking. (*People v. Fowzer* (1954) 127 Cal.App.2d 742.)

B. Computer Records Generated by a Mechanized Process

The first rule is that a printout of the results of the computer's internal operations is not hearsay evidence because hearsay requires a human declarant. (Evid.Code §§ 175, 225.) The Evidence Code does not contemplate that a machine can make a statement. (*People v. Goldsmith* (2014) 59 Cal.4th at 258, 274 [rejecting hearsay claims related to red light cameras]; *People v. Hawkins* (2002) 98 Cal.App.4th 1428; *People v. Lopez* (2012) 55 Cal. 4th.569). These log files are computer-generated records that do not involve the same risk of observation or recall as human declarants. Thus, email header information and log files associated with an email's movement through the Internet are not hearsay. The usual analogy is that the clock on the wall and a dog barking are not hearsay. An excellent discussion on this issue can be found in *Chapter 5 – Evidence* of the United States Department of Justice, Computer Crime and Intellectual Property Section Criminal Division, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (2009) <http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf> (accessed Aug. 18, 2016) Metadata such as date/time stamps are not hearsay nor do they violate the confrontation clause because they are not testimonial. (See, *People v. Goldsmith* 59 Cal.4th at 258, 274-275; *People v. Lopez* (2012) 55 Cal. 4th.569, 583.)

C. Business Records

Log files and other computer-generated records from Internet Service Providers may also easily qualify under the business records exception to the hearsay rule. (Evid.Code §§1270, 1271, 1560, 1561.) Remember, you do not need to show the reliability of the hardware or software. (*People v. Lugashi* (1988) 205 Cal.App.3d 632.) Nor does the custodian of records need to completely understand the computer. (*Id.*) Additionally, the printout (as opposed to the entry) need not be made "at or near the time of the event." (*Aguimatang v. California State Lottery* (1991) 234 Cal.App.3d 769.) Finally, a cautionary note from the Appellate Court in *People v. Hawkins* (2002) 98 Cal.App.4th 1428: "the true test for admissibility of a printout reflecting a computer's internal operations is not whether the printout was made in the regular course of business, but whether the computer was operating properly at the time of the printout."

If the computer is used merely to store, analyze, or summarize material that is hearsay in nature, it will not change its hearsay nature and you will need an applicable exception for introduction. Common exceptions for the contents of email include: statement of the party, adoptive admission, statement in furtherance of a conspiracy, declaration against interest, prior inconsistent statement, past recollection recorded, business record, writing as a record of the act, or state of mind.

Note also that records obtained by search warrant, and accompanied by a complying custodian affidavit, are admissible as if they were subpoenaed into court (Evid. Code §§ 1560-1561, effective January 1, 2017) and records obtained from an Electronic Communication Service provider that is a foreign corporation, and are accompanied by a complying custodian affidavit, are currently admissible pursuant to Penal Code § 1524.2(b)(4). (See also Pen. Code § 1546.1(d)(3).)

D. Government Records

An official record is very similar to a business record, even if it is obtained from a government website. The chief difference is that it may be possible to introduce an official record without calling the custodian or another witness to authenticate it. (Evid. Code, § 1280; See *Lorraine v. Markel American Ins. Co.* (D. Md. 2007) 241 F.R.D. 534, 548–49; *EEOC v. E.I dupont de Nemours & Co*. (2004) 65 Fed. R. Evid. Serv. 706 [Printout from Census Bureau web site containing domain address from which

image was printed and date on which it was printed was admissible in evidence].) The foundation can be established through other means such as judicial notice or presumptions. (*People v. George* (1994) 30 Cal.App.4th 262,274.)

E. Published Tabulations

Prosecutors are often plagued with how to introduce evidence that was found using Internet-based investigative tools. For example, if your investigator used the American Registry For Internet Numbers (ARIN) programs (WHOIS, RWhois or Routing Registry Information), how is this admissible without calling the creator of these Internet databases? Evidence Code Section 1340 allows an exception to the hearsay rule, which allows the introduction of published tabulations, lists, directories, or registers. The only requirement is that the evidence contained in the compilation is generally used and relied upon as accurate in the course of business.

Note that not all data aggregation sites may have the proper characteristics for this exception. In *People v. Franzen* (2012) 210 Cal.App.4th 1193, 1209–13, the court found that a subscription based service did not possess the characteristics that would justify treating its contents as a published compilation for purposes of section 1340

IV. Former Best Evidence Rule

Reminder: The Best Evidence Rule has been replaced in California with the Secondary Evidence Rule. The Secondary Evidence Rule allows the admissibility of copies of an original document. (Evid. Code, § 1521.) They are not admissible, however, if "a genuine dispute exists concerning material terms of the writing and justice requires the exclusion," or if admitting the evidence would be "unfair." (Evid. Code, § 1521.)

In a criminal action it is also necessary for the proponent of the evidence to make the original available for inspection at or before trial. (Evid. Code, § 1522.) For email or any electronic document, this is especially important, given the wealth of information contained in its electronic format, as opposed to its paper image.

Of interest, Evidence Code Section 1522 requires that the "original" be made available for inspection. Evidence Code Section 255 defines an email "original" as any printout shown to reflect the data accurately. Thus, the protections offered by Evidence Code Section 1522 are stripped away by Evidence Code Section 255. This is where the protections of Evidence Code Section 1521 are invoked: "It's unfair, your Honor, not be able to inspect the email in its original format."

Also, remember that Evidence Code Section 1552 states that the printed representation of computer information or a computer program is presumed to be an accurate representation of that information. Thus, a printout of information will not present any "best evidence rule" issues absent a showing that the information is inaccurate or unreliable.

Oral testimony regarding the content of an email [writing] is still inadmissible absent an exception. (Evid. Code, § 1523.) Exceptions include where the original and all the copies of the document were accidentally destroyed.

Of course, none of the above rules applies at a preliminary hearing. (*See* Pen. Code § 872.5 [permits otherwise admissible secondary evidence at the preliminary hearing]; B. Witkin, 2 California Evidence (3rd ed., 1986) § 932, p. 897 ["secondary evidence" includes both copies and oral testimony].)

[1] This material was prepared by Robert M. Morgester, Senior Assistant Attorney General, California Department of Justice in 2003 for the *High-Technology Crime: Email and Internet Chat Resource CD-ROM*, and draws heavily upon *Documentary Evidence Primer*, by Hank M. Goldberg, Deputy District Attorney, Los Angeles County District Attorney's Office, January 1999. Material from that document was used with Mr. Goldberg's permission. This material was updated in 2016 by Robert Morgester and Howard Wise, Senior Deputy District Attorney, Ventura County District Attorney's Office.

How does Hearsay Play into the Era of Text Messaging?

With the ubiquitousness of smart phones, text messages have now become a preferred tool of communication for many. Due to the informal nature of text messages, many, if not most people fail to consider the potential evidentiary effect of a text message. As a general proposition, despite the informal usage of text messages, a text message can potentially still be evidence in the case, subject to the rules of hearsay, with further caveats. In this post, we specifically discuss how the lack of response to a text messages cannot qualify as an adoptive admission as an exception to the hearsay rule.

Hearsay evidence in Trial

The concept of "hearsay" as it pertains to trial is well known. As many people know, out of court statements offered for its truth are barred by the hearsay rule due to inherent trustworthiness and reliability concerns. However, there are many exceptions to this rule that would allow an otherwise inadmissible statement to be offered as evidence or for some other purpose in court. One major exception to the hearsay rule are admissions made by a party.

ALSO READ Why a Lis Pendens is Important in Specific Performance Claims

Admissions Made by a Party

Specifically, an admission for the purposes of the hearsay exceptions in any out of court statement or assertive conduct by a party to the action that is inconsistent with a position the party is taking at current proceeding. The statement itself does not necessarily need to have been against the party's interest when it was made. Indeed, even a statement self-serving whenmade may be admissible as a party admission if contrary to the party's present position at trial. (*People v. Richards* (1976) 17 Cal.3d 614, 617-618 (disapproved on other grounds by *People v. Carbajal* (1995) 10 Cal.4th 1114, 1126.)

Notably, an admission does not necessarily require an affirmative statement by the party taking the inconsistent position. Indeed, silence may be treated as an adoptive admission if, under the circumstances, a reasonable person would speak out to clarify or correct the statement of another were it untrue. (*People v. Riel* (2000) 22 Cal.4th 1153, 1189.) However, silence is not admissible as an adoptive admission if another reasonable explanation can be demonstrated. Indeed, in the recent case of *People v. McDaniel* (2019) 38 Cal.App.5th 986, 999 ("McDaniel"), the Court of Appeal held that failure to respond to a text message accusing defendant of committing a crime was not admissible as an adoptive admission.

ALSO READ How to Win Attorneys' Fees in HOA Cases

In McDaniel, the prosecution attempted to use the defendant's mother's statement to show an adoptive admission by the defendant because the defendant did not text his mother back to deny her indirect accusation that he had committed several local robberies. The Court of Appeal rejected that theory. As the Court of Appeal explained, given the nature of text messaging, the fact that the defendant did not text his mother back was not sufficient to show he had adopted his mother's statement:

Text messaging is different from in person and phone conversations in that text exchanges are not always instantaneous and do not necessarily occur in "real time." Rather, text messages may not be read immediately upon receipt and the recipient may not timely respond to a text message for any number of reasons, such as distraction, interruption, or the press of business. Furthermore, people exchanging text messages can typically switch, relatively quickly and seamlessly, to other forms of communication, such as a phone call, social-media messaging, or an in-person discussion, depending on the circumstances. In short, in light of the distinctive nature of text messaging, the receipt of a text message does not automatically signify prompt knowledge of its contents by the recipient, and

furthermore, the lack of a text response by the recipient does not preclude the possibility that the recipient responded by other means, such as a phone call.

https://schorr-law.com/role-of-hearsay-in-the-era-of-text-messages/

TEXTS AS EVIDENCE: ELECTRONICALLY STORED INFORMATION IN COURT

ARE TEXT MESSAGES ADMISSIBLE IN COURT? AFTER AN ACCIDENT THE OTHER DRIVER ADMITTED SHE WASN'T PAYING ATTENTION. IN A TEXT LATER THE DRIVER SAID SHE WAS SORRY, THAT SHE'D BEEN ON THE CELL PHONE, AND OFFERED TO PAY OUTSIDE OF INSURANCE. NOW THAT HER INSURANCE COMPANY IS INVOLVED SHE DENIES EVERYTHING. IS THE TEXT ADMISSIBLE IN COURT?

If you watch those TV court shows you may have seen them admit texts without a thought. Remember they have to get everything in between the commercials.

In an actual court of law electronically stored information, or "ESI", faces several tests under the rules of evidence.

ESI includes texts, emails, chat room conversations, websites and other digital postings. In court, admitting ESI requires passing these steps:

1. Is the electronic evidence relevant?
2. Can it pass the test of authenticity?
3. Is it hearsay?
4. Is the version of ESI offered the best evidence?
5. Is any probative value of the ESI outweighed by unfair prejudice?

The text must pass each step. Failing any one means it's excluded. Proving relevance poses a relatively simple challenge. But meeting the authenticity requirement raises larger questions.

Establishing the identity of the sender of a text is critical to satisfying the authentication requirement for admissibility. Showing the text came from a person's cell phone isn't enough. Cell phones are not always used only by the owner.

Courts generally require additional evidence confirming the texter's identity. Circumstantial evidence corroborating the sender's identity might include the context or content of the messages themselves.

HEARSAY RULE AND ELECTRONICALLY STORED INFORMATION

Text messages and other ESI are hearsay by nature. The hearsay rule blocks admission of out of court statements offered to prove the truth of the matter at issue. But court rules, which vary from jurisdiction to jurisdiction, are full of exceptions and definitions of "non hearsay".

Here, the text by the other driver that she wasn't paying attention at the time of the car accident should qualify as an admission, a prior statement by the witness or a statement by a party opponent.

TEXTS AND 'BEST EVIDENCE' RULE

Two more layers remain in the evidentiary hurdle. ESI presents its own challenges in passing the 'best evidence rule' or the 'original writing rule'. Essentially the rules require introduction of an original, a duplicate original or secondary evidence proving the version offered to the court is reliable.

The final test requires that the probative value of the evidence not be outweighed by considerations including unfair prejudice, confusion of the issues or needless presentation of cumulative evidence.

ESI AND TEXTS AS EVIDENCE: WHY SO HARD?

Sometimes the challenge isn't as overwhelming as it seems. In a federal case in which I was involved the court addressed all five steps of the process in ten minutes and admitted a series of texts. But a federal magistrate in Maryland wrote a 101 page decision thoroughly detailing the above process, rejecting some emails.

These are the evidence issues confronting texts and any electronically stored information. But, people who fail to object to evidence waive their right to object later, including upon appeal. Evidence of all kinds sometimes sneaks in despite the rules. So, go through the analysis long before running up the courthouse steps.

https://attorney-myers.com/2014/05/texts-as-evidence/

Electronic Communication

Text Messages

Text Messages

- **You need to PRINT!!! Court will not allow you to admit a phone so either:**
  - Email the messages to your email;
  - Take a screenshot of the conversations and email the screenshots to your email and print (make sure the screenshots are in order of messages were received!!)
  - The phone company may print out messages for a specific number (this option may not be available if the messages were sent months/years before)

Examples of Screenshot

Foundational Questions

Email

Q: Do you recognize the document that I have just shown you?

A: Yes I do.

Q: What is it?

A: It's an email conversation.

Q: From who was the email from and who was it addressed to?

A: It was from me to John.

Q: What did the email state?

A: In the email I had written that I was not going to allow my children to see him anymore because my children had come home with bruises on their arms and legs and had told me that their dad had beaten them when he had gotten drunk.

Q: Is this something that had happened on a previous occasion?

A: Yes, it had happened on two other occasions and I had also included that in the email.

Q: How do you know he was actually beating the children and they just weren't getting injured outside playing?

A: Because he used to beat me and my children when he would get into his drunken rages. That's why I left!!!

The (Ubiquitous) Email

- Insert email conversation video.

Electronic Communications

Emails

Emails

- Print the email and make sure that it includes the **sender, recipient, and important dates for identification purposes.**
- Then follow the standard steps for admitting a writing

Outlook Calendar People Tasks ...

Martinez < @gmail.com>

He became a sex offender for mooning? How childish? How can you bring our kids around someone who h
made such poor choices? And as for the porn, our kids don't even know what porn is so how can they say I
it out!?!? And I would never drive our children around without them being in their seat!! Our neighbor is lyi
Can they, or you even prove that had happened? I know our kids were in their seats and if your going to
believe our neighbor off of what they "saw" than that's your own problem. You'll never take my kids away fr
me!

REPLY REPLY ALL FORWARD

Carlson

To: @gmail.com

JOHN,

YOU CLAIMED THAT MY NEW BF IS ON SEXOFFENDER.COM BUT WHAT YOU DONT KNOW IS THAT PEOPLE CA
BECOME SEX OFFENDERS FOR MOONING PEOPLE OR PEEING IN PUBLIC WHICH IS WHAT ALEX DID. HE WAS 1
AND MOONED SOMEONE AND A COP CITED HIM. BUT YOU HAVE NO EXCUSE FOR THE PORN YOU LEFT OUT
THE TABLE THAT OUR CHILDREN FOUND. OUR CHILDREN TOLD ME ABOUT THOSE DAMN MAGAZINES AND
MOVIES WHICH YOU ALWAYS TRIED TO HIDE FROM ME.... AND DRIVING OUR KIDS WITHOUT THEIR CAR
SEATS!!! OUR NEIGHBOR TOLD ME ALL ABOUT HOW HE SAW YOU DRIVING OUR KIDS AROUND WITHOUT CA
SEATS. YOU CLAIM IM THE BAD PARENTS WELL IM TAKING YOUR KIDS AWAY FOR GOOD THIS TIME.

Electronic Communications

Video Recordings and Voicemails

Video Recordings

- If a video is on a phone, it needs to be transferred off the phone for review by the opposing party and court.
- It would also need to be transcribed into words along with a copy of the recording for review.
- If you plan to use a digital exhibit, video-taped depositions, or an overhead projector, the court should be advised at the earliest opportunity.
- It is Counsel's responsibility to supply the necessary equipment and to have it set up before trial or during recess.

Voicemails

- It needs to be transcribed into words. The transcript and recording must be provided to the opposing party for review.

Testimonial Evidence vs. Real Evidence

- Keep in mind that you don't need real evidence, like screenshots or text message transcripts, to use social media evidence.
- Social media can be introduced using testimonial evidence as long as the witness testifying about the social media:
  - Has personal knowledge of the social media information;
  - Has the ability to communicate the testimony;
  - Takes an oath or makes an affirmation to tell the truth; and
  - Claims to recall what they are testifying.

Foundational Questions
Photos

Q: Mrs. White, I'm showing you Plaintiff's exhibit #1. Do you recognize the scene in the photograph?

A: Yes

Q: What does the scene show?

A: It shows the corner of Maple and Amber where the accident occurred.

Q: Does this photo fairly and accurately show how that intersection looked at the time of the accident?

A: Yes it does.

Q: Your Honor, we offer Plaintiff's Exhibit #1 into evidence.

(At this time, the court will ask if there are any objections, if none then admitted.)

The Photograph Video

- Insert street corner photograph video.

Electronic Communications

Photos

Photos

- Print the photos and present to the other side for examination;
- Set up the foundation for the photo; and
- Have it marked by the court before admitting into evidence.

Electronic Communications

Editing is All Too Easy!

Electronic Communications

Presenting the Evidence

- Some ways of turning a electronic communication into hard copy:
  1. Print the page if printing is available;
  2. Send picture to email, then print;
  3. Screenshot the information (i.e. Facebook page, Instagram photos or text messages) and email to your account then print.
     - For a phone: Google how to screenshot for that particular phone.
     - For a computer: Depends on PC or Mac.

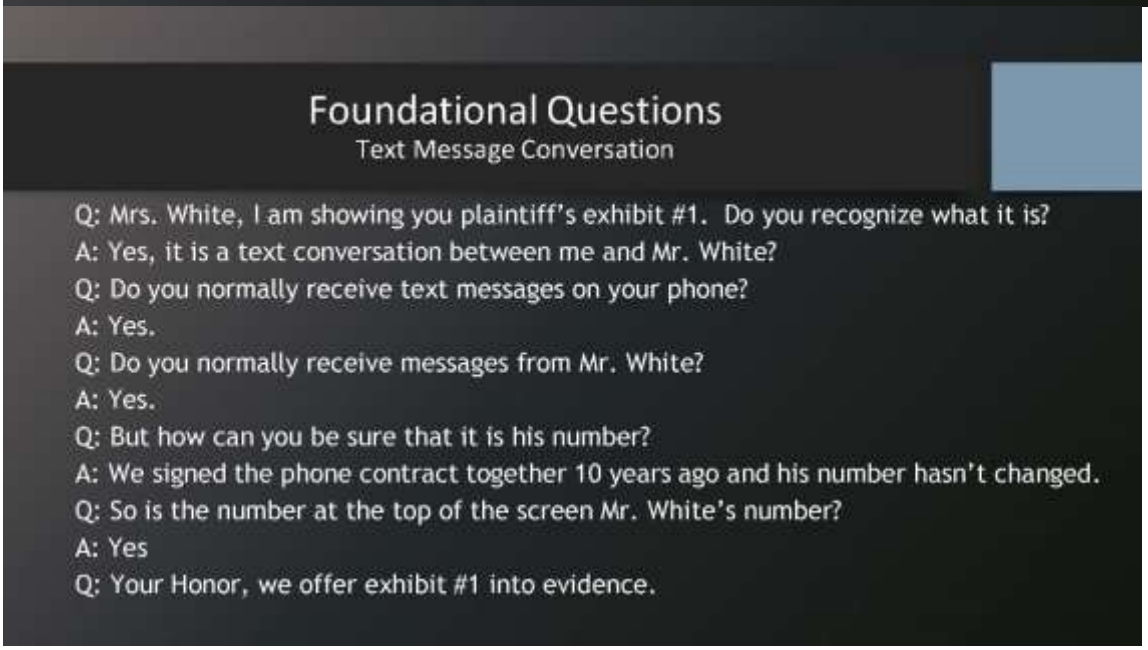
EXAMPLE - Screenshots

Electronic Communications

General

- **Electronic Communications include text messages, video recordings and pictures, voicemails and Facebook pages, and Instagram pictures.**

PROBLEM!!! You cannot just hand over a phone or computer. The information that is being presented needs to be printed so it can be presented in court to both the judge and opposing counsel.



CITED
https://www.courts.ca.gov/partners/documents/admittingsocialmediaEvidencePPT.pptx

Cal. Evid. Code § 1414

Section 1414 - Admissions of authenticity

(a) The party against whom it is offered has at any time admitted its authenticity; or

(b) The writing has been acted upon as authentic by the party against whom it is offered.

Ca. Evid. Code § 1414

Enacted by Stats. 1965, Ch. 299.

The Georgia Supreme Court ruled on 11/7/2016 that outgoing text messages found in a cell phone are admissible in evidence as admissions of the person who sent them. However, incoming text messages are inadmissible hearsay, though their admission in evidence was "harmless" under the circumstances of the case. *Elispie v. State*, decided November 7, 2016.
This ruling arose in the context of the criminal prosecution of an alleged drug dealer. That would have been a great interest in my past life as a prosecutor, though of course cell phones had not been invented when I was sending criminals to prison.

Text messages can be obtained by law enforcement with a search warrant based upon probable cause to examine the contents of a cell phone. If I were still a prosecutor, I would probably seek search warrants for contents of cell phones in a lot of cases.

In the civil context, however, we do not have that option. We cannot get search warrants in civil cases. Cell phone service providers, e.g., AT&T, Verizon, etc., typically do not keep text messages in the system more than perhaps 72 hours.

The only way to obtain those in a civil case is to obtain a court order for a forensic download of the phone. In addition to records of voice calls placed and received (though not the content of the calls, and text messages, forensic examination of wireless devices such as cell phones can reveal patterns of conduct and communication, including the times that the driver was using an app, typing a text, or watching a video. It has location history for the phone, showing where the driver was at various points in time. It includes calls, texts and emails between the driver and the trucking company. It may include records of communications with employer personnel inconsistent with prudent driver supervision by a motor carrier regarding fatigue management.

Parties opposing forensic download of a cell phone may assert claim of personal privacy. However, where the cell phone user killed someone, that fact may outweigh personal privacy. A trial court judge would be justified in ordering the download subject to a protective order limiting delicate personal information to use in the case after *in camera* review by the court.

THIS STATE OF GEORGIA RECOGNIZES THE COMLEXITY OF LEGITIMACY AND HOW IT CAN IMPACT FREEDOM IS IT IS SPOOFED BY SOMEONE AND LEAD TO IMPROPER PROSECUTION

(Rodriguez v. State (2012) 128 Nev. Adv. Op. 14, [273 P.3d 845].)

https://law.justia.com/cases/nevada/supreme-court/2012/56413.html

After a seven-day jury trial, Kevin Rodriguez was found guilty of multiple criminal counts. Rodriquez appealed, arguing that the district court erred
(1) in overruling his objection to the admission of twelve text messages because the State failed to authenticate the messages and the messages constituted inadmissible hearsay, and
(2) in overruling his objection to the admission of DNA non-exclusion evidence because the evidence was irrelevant without supporting statistical data.

The Supreme Court affirmed, holding that the district court
(1) abused its discretion in admitting ten of the twelve text messages because the State failed to present sufficient evidence corroborating Appellant's identity as the person who sent the ten messages, but the error was harmless; and
(2) did not abuse its discretion by admitting the relevant DNA non-exclusion evidence because, so long as it is relevant, DNA non-exclusion evidence is admissible because any danger of unfair prejudice or of misleading the jury is substantially outweighed by the defendant's ability to cross-examine or offer expert witness evidence as to probative value.

This is yet another STATE SUPREME that clearly understands how text can be manipulated

I want you to duly note that after finding this I did more digging and California already thinks this way

F. Authenticating Texts: A text message is a writing within the meaning of Evidence Code section 250, which may not be admitted in evidence without being authenticated.
(Stockinger v. Feather River Community College (2003) 111 Cal.App.4th 1014, 1027–1028.)

A text message may be authenticated "by evidence that the writing refers to or states matters that are unlikely to be known to anyone other than the person who is claimed by the proponent of the evidence to be the author of the writing"
(Evid.Code, § 1421), or by any other circumstantial proof of authenticity (Id., § 1410).
As of August 2016, there are no published California cases that specifically discuss what is required for authenticating a text message. Unpublished California opinions are consistent with the rule set forth above for authenticating e-mails and chats through a combination of direct and circumstantial evidence based on the facts of the case. Because of the mobile nature of smart phones, the proponent must take care to tie the declarant to the phone from which texts were seized or to the phone number listed in records obtained from the phone company. Often this done through cell phone records or the phone being seized from the defendant, his home or car or other witnesses testifying that this was how they communicated with the defendant. Published opinions from other jurisdictions and unpublished opinions from California provide some guidance:

Introducing Digital Evidence in California State Courts

• Victim testified he knew the number from which text was sent because Defendant told him the number. The contents of the texts referred to victim as a snitch. The defendant called the victim during the course of the text message conversation. [(Butler v. State, 459 S.W. 3d 595 (Crim. Ct App. Tx. April 22, 2015].)

• Testimony of records custodian from telecommunications company, explaining how company kept records of actual content of text messages, the date and time text messages were sent or received, and the phone number of the individuals who sent or received the messages, provided proper foundation for, and sufficiently authenticated, text messages admitted into evidence in trial on armed robbery charges. (Fed.Rules Evid.Rule 901(a), U.S. v. Carr (11th Cir. 2015) 607 Fed.Appx. 869.)

• Ten of 12 text messages sent to victim's boyfriend from victim's cellular telephone following sexual assault were not properly authenticated to extent that State's evidence did not demonstrate that defendant was author of text messages. (Rodriguez v. State (2012) 128 Nev. Adv. Op. 14, [273 P.3d 845].)

• Murder victim's cell phone recovered from scene of crime. Forensic tools used on phone recovered texts back and forth between victim and defendant. (People v. Lehmann (Cal. Ct. App., Sept. 17, 2014, No. G047629) 2014 WL 4634272 [Unpublished].)

• Defendant laid an inadequate foundation of authenticity to admit, in prosecution for assault with a deadly weapon, hard copy of e-mail messages (Instant Messages) between one of his friends and the victim's companion, as there was no direct proof connecting victim's companion to the screen name on the e-mail messages. (People v. Von Gunten (2002 Cal.App.3d Dist.) 2002 WL 501612. [Unpublished].) G. Authenticating Metadata: Another way in which electronic evidence may be authenticated is by examining the metadata for the evidence. Metadata, "commonly described as 'data about data,' is defined as 'information describing the history, tracking, or management of an electronic document.'

Metadata is 'information about a particular data set which describes how, when and by whom it was collected, created, accessed, or modified and how it is formatted (including data demographics such as size, location, storage requirements and media information).' Some examples of metadata for electronic documents include: a file's name, a file's location (e.g., directory structure or pathname), file format or file type, file size, file dates (e.g., creation date, date of last data modification, date of last data access, and date of last metadata modification), and file permissions (e.g., who can read the data, who can write to it, who can run it).

Some metadata, such as file dates and sizes, can easily be seen by users; other metadata can be hidden or embedded and unavailable to computer users who are not technically adept." Because metadata shows the date, time and identity of the creator of an electronic record, as well as all changes made to it, metadata is a distinctive characteristic of all electronic evidence that can be used to authenticate it under Federal Rule 901(b)(4). Although specific source code markers that constitute metadata can provide a useful method of authenticating electronically stored evidence, this method is not foolproof because, "[a]n unauthorized person may be able to obtain access to an unattended computer.

Moreover, a document or database located on a networked-computer system can be viewed by persons on the network who may modify it. In addition, many network computer systems usually provide authorization for selected network administrators to override an individual password identification number to gain access when necessary.

Metadata markers can reflect that a document was modified when in fact it simply was saved to a different location. Despite its lack of conclusiveness, however, metadata certainly is a 7 | Introducing Digital Evidence in California State Courts useful tool for authenticating electronic records by use of distinctive characteristics."

(Lorraine v. Markel American Ins. Co. (D. Md. 2007) 241 F.R.D. 534, 547–48 [citations omitted].) F. Challenges to Authenticity Challenges to the authenticity of computer records often take on one of three forms. First, parties may challenge the authenticity of both computer-generated and computer-stored records by questioning whether the records were altered, manipulated, or damaged after they were created. Second, parties may question the authenticity of computer-generated records by challenging the reliability of the computer program that generated the records. California state courts have refused to require, as a prerequisite to admission of computer records, testimony on the "acceptability, accuracy, maintenance, and reliability of ... computer hardware and software."

(People v. Lugashi (1988) 205 Cal.App.3d 632, 642.) As Lugashi explains, although mistakes can occur, " 'such matters may be developed on cross-examination and should not affect the admissibility of the [record] itself.' (People v. Martinez (2000) 22 Cal.4th 106, 132.) Third, parties may challenge the authenticity of computer-stored records by questioning the identity of their author. For further information, please consult "Defeating Spurious Objections to Electronic Evidence," by Frank Dudley Berry, Jr., or Chapter 5 – Evidence of the United States Department of Justice, Computer Crime and Intellectual Property Section Criminal Division, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations (2009) (accessed Aug. 18, 2016). III. Hearsay Rule The first question to ask is whether or not the information within the document is hearsay. If it is hearsay, then you need an applicable exception, such as business and government records or statement by party opponent. Examples of things that are not hearsay include; 1) operative facts and 2) data that is generated by a mechanized process and not a human declarant and, 3) A statement being used to show its falsity not its truth.

https://www.iap-association.org/getattachment/Conferences/Regional-Conferences/North-America-and-Caribbean/4th-North-American-and-Caribbean-Conference/Conference-Documentation/4NACC_Jamaica_WS1B_Morgester_CA-Digital-Evidence.pdf.aspx#:~:text=provided%20by%20statute.-,(Evid.,number%20that%20received%2C%20the%20text.

Why Would Someone Need to Authenticate Text Messages for Court?

In the contemporary age of technology, digital evidence is becoming increasingly important in court. Here is how to authenticate text messages for court in California.

Text messages are unfortunately a form of digital media that can easily be photoshopped and manipulated. This puts the evidence at risk of interference or invalidity. Additionally, text messages fall under the jurisdiction of California Evidence Code Section 250, which prevents any evidence from being used without first being authenticated.

Related: Can Text Messages Be Used in California Divorce Court?

How to Introduce Digital Evidence in California State Courts

Smartphones allow endless mobile communication that can be crucial evidence for a court case. In order to present documents and electronic evidence in a California state court, the accumulation of evidence must follow the California Electronic Communication Privacy Act (CPOA). The California Electronic Communication Privacy Act protects the privacy of individuals and their electronic devices, and it requires law enforcement to receive a warrant before they can access any electronic information.

To be in compliance with the CPOA, digital evidence must prove to be necessary for furthering the case. Additionally, in order to be sustainable in court, digital evidence must meet the following four components:

1. It must be relevant.
2. It must be authenticated.
3. Its contents must not be inadmissible hearsay (able to be disproven as fake).
4. It must withstand a "best evidence" objection.

Proposed digital evidence must meet the standards of both the CPOA and the four aforementioned components. The only exceptions to the protection of privacy that the CPOA ensures are if the individual gives consent or if the exception qualifies as an emergency situation. In order to meet the requirements of an emergency circumstance, the government entity must "in good faith, believe that an emergency involving danger of death or serious physical injury to any person requires access to the electronic device information" (CPOA).

Additionally, if the evidence contains metadata, the proponents must address the metadata separately. Metadata is data about the date, for example, a time

stamp on a screenshot in a text message. The proponents would need to consider the time and prepare an additional foundation for it.

The Four Components of Evidence Required Getting Authentication of Text Messages

Relevance is determined by the evidence's ability to prove or disprove any disputed fact, including credibility. In order for digital evidence to qualify as relevant, the defendant must usually be tied to the evidence being presented. Specifically, the proponent must be able to make a connection between the defendant and either the phone number that sent or received the text. Authentication of evidence requires the proponent to introduce sufficient evidence to hold that the writing is what they are claiming it is. To authenticate a text message it must hold that "by evidence the writing refers to or states matters that are unlikely to be known to anyone other than the person who is claimed by the prominent of the evidence to be the author of the writing." California Evidence Code Section 1421.

There are no published California cases that distinctly lay out the requirements for authenticating a text message, but unpublished California opinions are consistent with the rules set for authenticating emails and chats. This includes a combination of both direct and circumstantial evidence. Here are some examples of unpublished opinions from California:

- The murder victim's cell phone was recovered from the scene of the crime. The forensic tools used on the phone recovered the texts back and forth between victim and defendant. (People v. Lehmann (Cal. Ct. App., Sept. 17, 2014, No. G047629) 2014 WL 4634272 [Unpublished].)
- 10 of 12 text messages sent to the victim's boyfriend from the victim's cellular telephone following sexual assault were not properly authenticated to extent that the State's evidence did not demonstrate that the defendant was the author of the messages. (Rodriguez v. State (2012) 128 Nev. Adv. Op. 14, [273 P.3d 845].)

https://herlawyer.com/authenticate-text-messages-court/

Getting Authentication of Text Messages

For a text message to be used as evidence in California Divorce Court, it must be authenticated, meaning that the other party must admit to sending the message, a witness must testify that they have seen the message being created or reply authentication must be demonstrated. Reply authentication is demonstrated when a reply message is clearly sent in response to the original message.

The California Evidence Code also dictates ways in which electronic communications can be authenticated, such as if the message references something only the other party would know about or understand.

Authentication is important and necessary in the process of utilizing text messages in California Divorce Court because it verifies that the messages are legitimate evidence and not hearsay.

https://herlawyer.com/text-messages-divorce-court/

- he court reiterated the 5 step approach set forth by the U.S. Supreme Court in Neil v. Biggers 409 U.S. 188, 189 (1972) for determining the reliability of in-court voice identification: (1) the ability of the witness to hear the assailant speak, (2) the witness' degree of attention, (3) the accuracy of any prior identifications the witness made, (4) the period of time between the incident and the identification, and (5) how certain the witness was in making the identification.

Can Emails Be Used in Court?

Whether you are bringing or defending a business lawsuit, your litigation attorney has likely asked you to gather and organize relevant documents in preparation for your case. This involves anyone or any location that might have helpful information to confirm your argument.

Unfortunately, not all emails are admissible as evidence in a business litigation case. **Emails can be used as admissible evidence in a court of law if they're found to be authentic. Once they fit the criteria, the emails can be treated as legal documents.**

Determining Admissibility of Electronic Evidence

A business lawyer should help you determine which electronic communications are admissible and which are not, but we've described two main considerations here to get you started:

Message Must Be Authentic

It may be obvious to you that a specific email or text is the real deal and came from the source you claim. However, it's not overly difficult for someone with the right skillset to manipulate, fake, or corrupt digital data. For this reason;

- Your business litigation attorney must establish authenticity first and foremost.
- A litigator may gain authentication by deposing the sender or recipient of the email.
- When it comes to business litigation, company emails are normally considered self-authenticating when they:
    - contain official corporate identifiers, and
    - are confirmed by redundant records.

Content Must Be Reliable

Even if you can prove that the communication you received is authentic, that doesn't necessarily mean that its contents are helpful to your business lawsuit. The email in question could say the company is in breach of contract, but simply stating this, doesn't make it true. This is considered hearsay, whether spoken, emailed, or texted. Varying degrees of admissible evidence vs. hearsay could stem from a multi-email conversation depending on the nature of the content. Consequently;

- Your business attorney must prove the communication is an exception to the hearsay rule.
- In a business lawsuit, communication could be considered reliable when presented as:
    - **Business Record**:
        - the communication was created by an employer or officer of that company.
        - the communication was created by an employee of that company as one of their proven and regular official duties.
    - **Circumstantial Evidence**:
        - the communication confirms an event or timeline
        - the communication confirms relevant actions were taken
    - **Party Admission**:
        - the party in question is the creator/sender
        - the opposing part offered it into evidence
        - the communication was sent by a proven coconspirator

Of course, there are a variety of circumstances that could cause even emails that fall under these categories to become inadmissible. For example, if the sender was not in their right mind or if their motive is not expertly established, those emails will not hold up in court. Additionally, each state has its own laws surrounding the admissibility of electronic evidence, so the strength of your case is not always straight forward.

https://www.nwbizlaw.com/blog/2019/november/are-emails-admissible-as-evidence-in-a-business-/

a. Testimony by the Sender or a Recipient. Obviously the easiest way to authenticate a printout of an e-mail message is the testimony of the sender or a recipient (including a cc or bcc recipient)—a "Witness with Knowledge," under Rule 901(b)(1) of the Federal Rules of Evidence—whether by deposition or live at trial.

If the testimony is from a recipient of the message—or, for that matter, from a hostile witness who is identified in the message as its sender—proving the message (or overcoming post-admission arguments against its authenticity) may require testimony concerning the security of the sender's or organization's e-mail system under Rule 901(b)(9) (see below).

b. Testimony Concerning the E-Mail System, Process, and Servers. In the absence of testimony from the sender or a recipient, or if the sender disclaims the message, the authenticity of the message can be proven by appropriate testimony concerning the e-mail system or systems in question, under Federal Rule 901(b)(9) ("Evidence About a Process or System"), which requires evidence "describing a process or system and showing that it produces an accurate result."

The requisite testimony may be supplied by an expert witness, under Rule 702, or—especially if the e-mail message is internal, sent and received entirely within an organization's e-mail system—an information systems employee or officer of the organization, testifying as a fact witness or a lay opinion witness under Rule 701. If the purported sender isn't available or denies sending the message, the testimony will need to establish the reasons for believing that an e-mail sent from a particular address was in fact authored or forwarded by the person in question, addressing among other things the security of the system and access to the purported sender's computer or other device. [2]*See e.g.*, "Authentication of Electronically Stored Evidence, Including Text Messages and E-Mail," 34 A.L.R. 3d 253 (2008).

If the e-mail message in question was produced in discovery by the party opposing its admission, that fact alone typically clears the authenticity hurdle. [3]*See e.g.*, Pierre v. RBC Liberty Life Ins., Civ. A. No. 05-1042-C, 2007 BL 289606, at *1-2 (M.D. La. July 13, 2007).

Often testimony concerning the process that is sufficient to satisfy Rule 901(b)(9) will overlap with or be subsumed in testimony that the e-mail message constitutes a business record under Rule 803(6), discussed below.

2. Admissibility

After the printed e-mail message is authenticated, there remain hurdles to its admission into evidence. Even if the author of the message is on the stand authenticating it and admitting having sent it, the message remains hearsay, as a statement "that the declarant does not make while testifying at the current trial or proceeding …" under Rule 801(c)(1), if it is being "offered in evidence to prove the truth of the matter asserted in the statement." Rule 801(c)(2). It doesn't suffice that the witness reiterates the statement, word for word, from the witness stand; the e-mail message itself remains an out-of-court statement, and if offered to prove the truth of the matter asserted, it's inadmissible hearsay absent an applicable exception. So how do you make it admissible?

a. Not Offered for the Truth. Often the utility of an e-mail message doesn't turn on the truth, or falsity, of what's contained within its text. As mentioned earlier, e-mail messages provide a superb means of establishing the chronology of a dispute; you may not care whether the assertion is true, and indeed you may have reason to offer an opponent's or adverse witness's e-mail message while making clear that you dispute its veracity. For example, the message may simply demonstrate that at a crucial point in time, the opposing party was on notice of a position being taken by your client.

An e-mail message, like any other written or oral communication, isn't hearsay if it isn't being offered for the truth of its contents. But an assertion that this is the basis for admissibility can't be a subterfuge, and you obviously need to be able to articulate the non-hearsay reason why the message is relevant and what it tends to prove—and be willing to live with a limiting instruction informing the jury that the message can't be considered for its ostensible truth.

b. Opposing Party's Statement. Generally known under pre-Rules common law as "admissions of a party opponent," this concept is now codified in Rule 801(d)(2) as simply "An Opposing Party's Statement." Rule 801(d)(2) sets forth five alternative bases on which an e-mail message attributable to your opponent or its representative will be considered not hearsay, and thus will be admissible, including that the message evidences a statement that "was made by the party in an individual or representative capacity" (Rule 801(d)(2)(A)) or "was made by the party's agent or employee on a matter within the scope of that relationship and while it existed" (Rule 801(d)(2)(D)). For that matter, Rule 801(d)(2) at least holds out the possibility of admitting into evidence an e-mail message made by someone not associated with the party if it was accepted

and retained without comment—as "one the party manifested that it adopted or believed to be true." (Rule 801(d)(2)(B)).

Rule 801(d)(2) doesn't explicitly require that the e-mail message constitute an "admission," as the common law required, but if it's relevant under Rule 403—and if you're seeking its entry into evidence—there will presumably be something about the e-mail that's inconsistent with some aspect of your opponent's position at trial.

c. Declarant's or Witness's Prior Statement. In a similar vein, an e-mail message that was authored or adopted by a testifying witness and that is *consistent* with his trial testimony, doesn't constitute hearsay and is admissible under Rule 801(d)(1)(B) if offered to rebut a claim of recent fabrication or of testimony shaped by improper influence or motive.

d. Business Records. The business records (or "shop book") rule is codified in Rule 803(6) of the Federal Rules of Evidence ("Records of a Regularly Conducted Activity"). Since it falls within Rule 803's set of hearsay exceptions applicable regardless of whether the declarant is available, it's ideally suited for documents for which you *don't* have testimony from a sender or recipient.

Courts have repeatedly ruled that e-mail messages can constitute business records under Rule 803(6) or corresponding state law rules of evidence. [4]See DirecTV, Inc. v. Murray, 307 F. Supp. 2d 764, 772 (D.S.C. 2004); Canatxx Gas Storage Ltd. v. Silverhawk Capital Partners, LLC, Civ. A. No. H-06-1330, 2008 BL 98139, at *12-13 (S.D. Tex. May 8, 2008); Pierre v. RBC Liberty Life Ins. (M.D. La. July 13, 2007). For state court opinions see D.B. Zwirn Special Opportunities Fund L.P. v. Brin Inv. Corp., 945 N.Y.S.2d 556, 556 (N.Y. App. Div. 2012); Thomas v. State, 993 So.2d 105, 107 (Fla. Dist. Ct. App. 2008). The application of Rule 803(6) to e-mail messages does trigger some "unique problems of recent vintage." U.S. v. Cone, 714 F.3d 197, 219 (4th Cir. 2013). For example:

Who is the "custodian or other qualified witness" (Rule 803(6)(F))? Ordinarily (and to the extent the opposing party really wants to contest such matters) the custodian will be a person within the organization responsible for, or otherwise familiar with, its e-mail system and servers. Nowadays, however, the general acceptance of e-mail as a means of communication probably renders rare the circumstances in which opposing counsel will insist on trying the patience of jury, judge, or arbitrator by requiring detailed background testimony concerning e-mail technology.

Can an incoming e-mail message, from a sender not affiliated with the organization, nevertheless become a business record if incorporated into the organization's files? Conceivably a company's procedures could include the incorporation of incoming messages into its own records. Further, however, if an incoming message is thereafter forwarded by an employee of the organization under circumstances indicating adoption of its contents—a so-called "adoptive admission"—the message is admissible under Rule 801(d)(2)(B). [5]In re Oil Spill by the Oil Rig "Deepwater Horizon" in the Gulf of Mexico, MDL No. 2:10-md-02179-CJF-SS, 2012 BL 54760, at *5 (E.D. La. Jan. 11, 2012).

Under what circumstances is an e-mail message "kept in the course of a regularly conducted activity"? Courts seem less than uniform in their application of this requirement. For example, e-mail messages sometimes are used to make, and thereafter transmit, notes of a telephone conversation. One court, in ruling such an e-mail message admissible, observed that, "[I]t is reasonable that those in business meetings often keep notes of those meetings in the regular course of business …" and that in the instance then before the court, "[N]othing in the notes or testimony indicates that the conversation strayed in any way beyond a strictly business discussion." [6]Insignia Sys. Inc., News Am. Mktg. In-Store, Inc., Civil No. 04-4213 (JRT), 2011 BL 28726, at *8 (D. Minn. Feb. 3, 2011). Other courts appear to read a more rigorous standard into Rule 803(6), with e-mail messages not falling within Rule 803(6) unless the employer required the employee to make and maintain e-mails as part of his job duties. [7]*See, e.g.*, Canatxx Gas Storage Ltd., 2008 BL 98139, at *12-13; In re Oil Spill by the Oil Rig "Deepwater Horizon" in the Gulf of Mexico, MDL No. 2:10-md-02179-CJF-SS, 2012 BL 54760, at *6 (E.D. La. Jan. 11, 2012) ("Essentially, there must be a showing that the e-mail at issue was not sent or received casually . . . .").

Is a snarky e-mail message concerning fellow employee (or opposing party) really part of the regular activity of the organization? It can be, if the court concludes that the message relates sufficiently to the sender's designated responsibilities—and, again, courts vary as to how rigorously they apply the Rule 803(6) standard on this point. If the message is sufficiently problematical and the adverse comment arguably tangential, there's always the possibility of arguing that prejudice outweighs probative value under Rule 403.

There are other issues, of course, that would justify an entire article about e-mail communications as business records.

e. Present Sense Impression. "A statement describing or explaining an event or condition, made while or immediately after the declarant observes it …" is admissible under Rule 803(1), regardless of whether the declarant is available to testify. This exception has been applied to justify the admission of, for example, an e-mail message concerning a just-finished telephone conversation with a representative of the opposing party. [8]Canatxx Gas Storage Ltd., 2008 BL 98139, at *14. This exception seems peculiarly adaptable given the dynamics of e-mail communication—virtually universal and immediate access to a computer, tablet, or smartphone, with which to inadvertently record for posterity what would in past times have existed only in non-electronic memory.

f. State of Mind. An e-mail message illustrating its sender's "then-existing state of mind … or emotional, sensory, or physical condition …" is admissible under Rule 803(3)—again, regardless of whether the sender is available to testify—in a case in which it is relevant.

C. E-MAIL MESSAGES AS TESTIMONIAL SUPPORT BUT NOT NECESSARILY ADMISSIBLE

There are at least two circumstances in which an e-mail message may be effective to bolster oral testimony but may *not* be admissible into evidence.

https://news.bloomberglaw.com/us-law-week/effective-use-of-e-mail-messages-in-witness-examination